TEMPERED NETWORKS®

Use Case

Infrastructure as Code: Multi-Cloud Micro-Segmentation

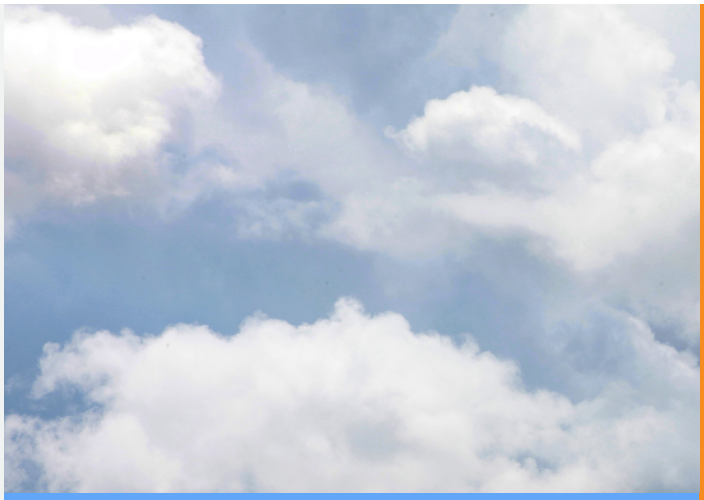
Programmable overlay networks make workloads invisible to unauthorized machines

What Our Hybrid and Multi-Cloud Customers Experience:

90% Reduced Attack Surface
through workload micro-segmentation

100% Elimination of Errors
that expose workloads to public Internet

100% Compatibility and Automation
with no changes to infrastructure



Challenge Overview – Complex Multi-Cloud Segmentation

The complexities and limitations of traditional IT solutions for multi-cloud micro-segmentation has left DevOps teams feeling exposed and dependent upon ineffective cloud security controls. All too often we've seen teams inadvertently expose workloads to the public Internet by a simple security group error or Internet gateway change.

When our customers sought to connect and micro-segment workloads and containers to protect applications and data between local resources, availability zones, regions and across cloud providers, they found native security controls not only ineffective and inconsistent, but too complex to maintain across environments. Attempting segmentation proved to be so error prone and unsustainable that workload connections were often mistakenly blocked. In order to remove downtime as a risk, loose security controls like enforcing access control based on IP address range and ports are used. Using non-verifiable access controls exposed our customers' workloads to spoofing exploits and lateral attacks.

Tempered Networks – Simple Software Defined Segmentation

Identity Defined Networking (IDN) creates a highly available, natively secure, and programmable overlay network for workloads across on-premise and multi-cloud environments. With infrastructure as code, our customers move the security and network perimeter from the network edge to the host, making policy orchestration explicit and programmable. Now they can deploy automated networking and access control for workloads that is as predictable as their build server environment. With Software-Defined Segmentation, protection is automated and workloads are made invisible to unauthorized machines, giving DevOps the agility and peace of mind they seek.

Network Challenges:

- Using IP addresses and ranges to restrict access prevents micro-segmentation
- Multi-cloud network dependencies impede simple and predictable connectivity
- Lack of infrastructure as code prevents network automation, orchestration, and predictability

Security Challenges:

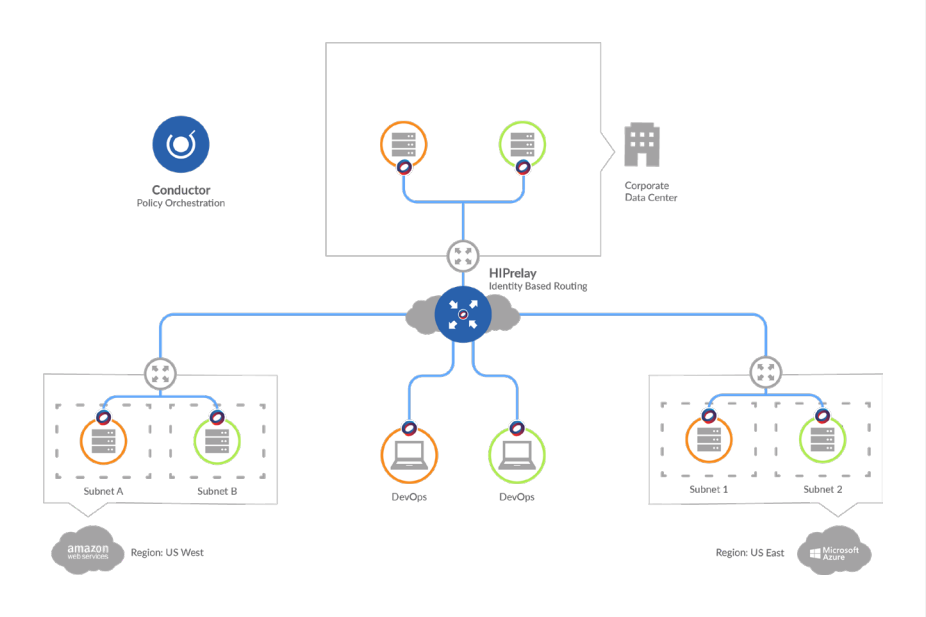
- Workloads exposed to lateral attacks in cloud subnets
- Root workload SSH exposure through key sharing
- Difficulty applying and maintaining consistent security controls across clouds

People and Process Challenges:

- Network configuration errors that impact agile and predictable workflows
- Lack of network and security programmability slows and exposes DevOps

"The inability to quickly micro-segment workloads across AWS and Azure zones, regions, and between our on-premises environment forced us to consider writing our own control plane at considerable time and cost. With Tempered Networks, we overcame those limitations and have significantly improved our release cycles. We now have greater predictability and confidence that our apps and data are locked down."

Director of Cloud and DevOps
Fortune 1000 Energy SaaS Provider



Challenges with Traditional IT Solutions

- Loose security controls due to lack of machine authentication to enforce access policy
- Inability to unify and peer segmented groups across the WAN and clouds
- Different automation and security enforcement controls across clouds
- Infrastructure dependency errors that expose apps and data to public Internet
- IP and connectivity conflicts caused by different cloud IP schemas
- Lack of centralized control to add, disable, move, and revoke machine access

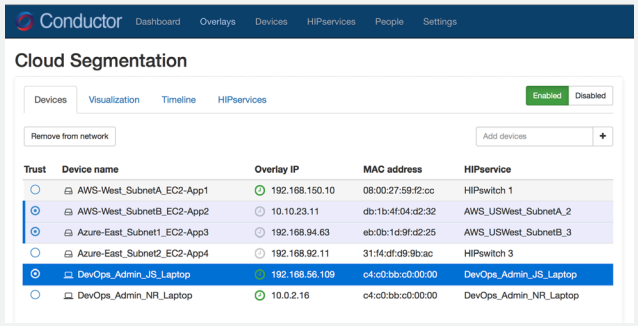
Native Security and Network Simplification with Tempered Networks

- Distributed workloads across clouds behave like one unified broadcast domain
- Authenticated and authorized AMI and VM access before data transport
- Network and security infrastructure as code for fast and simple micro-segmentation
- Private machine-to-machine peering (no public IP exposed) within and across clouds
- Native machine-to-machine encryption across LAN, WAN, and clouds
- Simple network automation to add, disable, move, or revoke machines in one click

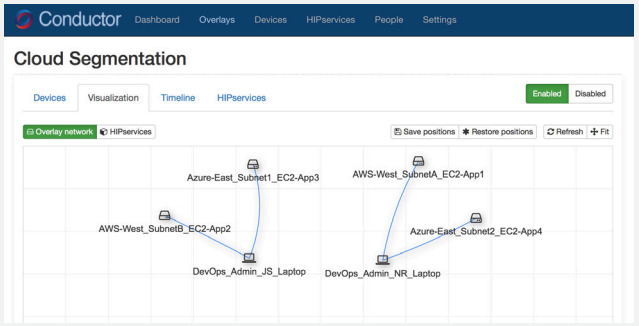
With IDN's infrastructure as code, DevOps teams eliminate network complexity and gain the freedom of mobility. Automating secured peering between machines or groups of machines without having to modify the underlying network infrastructure supports DevOps agility and reliability objectives. Programmable cloud network overlays result in simple infrastructure configuration and resiliency that can't be achieved using traditional IT solutions. Teams can now quickly connect, micro-segment, encrypt, and manage workload peering and access control based on verifiable machine identity, not ephemeral IP and ports.

Trust-Based Peering and Micro-Segmentation in Minutes

Tempered Networks' scalable orchestration engine was designed to be extremely easy to use with no advanced technical training, and is also programmable with a restful API. Unlike the many complex, fragile, and time-consuming steps associated with cloud networking and security, our customers eliminate human error through point-and-click policy orchestration. All network connections between workloads are automatically authenticated and authorized before session establishment and directly connected across any network. Every cloud workload can now remain private, segmented, and invisible to hackers - eliminating reconnaissance and spoofing attacks.



Trusted end-to-end connectivity with point-and-click simplicity to add, disable, and revoke machines.



The Visual Trust Map verifies creation and revocation of connectivity and segmentation between workloads.

Impacts of Traditional IT Solutions vs. Tempered Networks

The customer scenario below is based on isolating and securely peering the corporate network and 20 regionally distributed AWS VPCs and Azure VNETs. DevOps follows a typical build, test, and release workflow with all 50 members requiring discrete remote access from anywhere. Benefits do not include functions like cloaked micro-segmentation that would be impossible without developing a custom network data and control plane.

IMPACTS	TRADITIONAL IT SOLUTIONS	TEMPERED NETWORKS SOLUTION
ANNUAL SOLUTION COST	$220,000 +	$100,000
NET/SEC PROVISION TIME PER RELEASE	3 FTE DAYS	5 MINUTES
ADDITIONAL HEADCOUNT	6 CCNE LEVEL ADMINS	0 NEW ADMINS

*Traditional IT Solutions include: Firewalls, VPNs, Routers, Modems, VLANs, ACLs, NAC, Port Lockdown, etc

Have us prove it to you in less than 30 minutes.

Visit temperednetworks.com/segment-cloud to request a demo or call us at 206.452.5500

